Claims:

1. (Currently Amended) A computer-executable method, comprising:

via operations of a processor of a computing device,

intercepting a message at the computing device that modifies security information associated with an object, the security information identifying an owner of the object and an entity that has access to the object;

determining, at the computing device, if the owner exceeds a first threshold security level, and if so, issuing a first notification that the owner exceeds the threshold security level; and

determining, at the computing device, if the entity that has access to the object exceeds a second threshold security level, and if so, issuing a second notification that the entity exceeds the second threshold security level.

2. (Original) The method recited in claim 1, wherein the first threshold security level identifies the owner as being a questionable security risk.

3. (Original) The method recited in claim 1, wherein the first threshold security level identifies the owner as being a dangerous security risk.

4. **(Original)** The method recited in claim 1, wherein not exceeding the first threshold security level identifies the owner as being trusted.

5. **(Original)** The method recited in claim 1, further comprising determining if a grant of permissions to the entity exceeds a third security threshold, and if so, issuing a third notification that the grant of permissions exceeds the third security threshold.

6. **(Original)** The method recited in claim 5, wherein the grant of permissions comprises information that describes what access to the object for which the entity is authorized.

7. **(Original)** The method recited in claim 1, wherein the security information is embodied in a security descriptor associated with the object.

8. **(Original)** The method recited in claim 7, wherein the security descriptor further comprises an owner field having a security identifier that identifies a security context associated with the owner.

9. (Original) The method recited in claim 7, wherein the security descriptor further comprises a Discretionary Access Control List containing the information about the entity that has access to the object.

10. (Original) The method recited in claim 9, wherein the information about the entity comprises a security identifier that identifies a security context of the entity, and an access mask that defines permissions granted to the entity.

11. (Original) The method recited in claim 1, wherein intercepting the message comprises hooking an Application Programming Interface (API) that enables the modification to the security information.

12. (Canceled)

13. (Currently Amended) A computer-readable medium having computer-executable instructions embodied thereon, the computer-executable instructions when executed on one or more processors configuring the one or more processors to perform acts comprising:

~~for~~ evaluating a security threat posed by an application modifying an object, via ~~the instructions~~ operations comprising:

intercepting a modified security descriptor for an object, the security descriptor including an owner SID field and a DACL, the owner SID field

identifying an owner of the object, the DACL identifying at least one entity that has access to the object and access permissions for the entity;

evaluating the owner of the object to determine if the owner is categorized as dangerous, and if so, issuing an alert notification;

evaluating the DACL to determine if the entity is categorized as dangerous, and if so, issuing the alert notification; and

if the entity is not categorized as trusted, evaluating the DACL to determine if the access permissions for the entity are categorized as dangerous, and if so, issuing the alert notification.

14. (Currently Amended) The computer-readable medium recited in claim 13, wherein the acts further ~~comprising~~ comprise evaluating the owner of the object to determine if the owner is categorized as questionable, and if so, issuing a warning notification.

15. (Currently Amended) The computer-readable medium recited in claim 13, wherein the acts further ~~comprising~~ comprise evaluating the DACL to determine if the entity is categorized as questionable, and if so, issuing a warning notification.

16. (Currently Amended) The computer-readable medium recited in claim 13, wherein the acts further ~~comprising~~ comprise evaluating the DACL to

determine if the access permissions are categorized as questionable, and if so, issuing a warning notification.

17. (Currently Amended) The computer-readable medium recited in claim 13, wherein the notification comprises a ~~substantially instantaneous~~ an immediate notice issued to a user.

18. (Original) The computer-readable medium recited in claim 13, wherein the notification comprises an entry in a log.

19. (Currently Amended) A computer-readable medium having computer-executable components embodied thereon, the computer-executable components executable on one or more processors to configure the one or more processors to perform acts comprising:

intercepting a message that affects security information of an object by a security verifier having a security descriptor evaluator component configured to intercept [[a]] the message that affects security information of an object, and

evaluating, by the security verifier ~~to evaluate~~ a security identifier associated with an entity having access rights to the object, the evaluation including a determination whether the entity is categorized as other than trusted, the security descriptor evaluator component being further configured to issue a notification if the entity is categorized as other than trusted.

20. (Original) The computer-readable medium recited in claim 19, wherein the security descriptor evaluator component is further configured to issue a second notification if the entity is categorized as dangerous.

21. (Original) The computer-readable medium recited in claim 19, wherein the security descriptor evaluator component is further configured to evaluate a second security identifier associated with an owner of the object, and to issue a notification if the owner is categorized as other than trusted.

22. (Original) The computer-readable medium recited in claim 21, wherein the security descriptor evaluator component is further configured to issue a second notification if the owner is categorized as dangerous.

23. (Original) The computer-readable medium recited in claim 19, wherein the security descriptor evaluator component is further configured to evaluate the access rights of the entity, and to issue a notification if the access rights are categorized as other than safe.

24. (Original) The computer-readable medium recited in claim 23, wherein the security descriptor evaluator component is further configured to issue a second notification if the access rights are categorized as dangerous.

25. (Original) The computer-readable medium recited in claim 19, wherein the security information is contained in a security descriptor associated with the object.

26. (Original) The computer-readable medium recited in claim 25, wherein the security identifier is contained within a DACL.

27. (Original) The computer-readable medium recited in claim 26, wherein the access rights are described in the DACL.

28. (New) The method recited in claim 1 wherein:

interception of the message launches an application in a controlled execution environment;

the owner is categorized into one of a plurality of risk categories;

the entity is categorized into one of a plurality of trust types such that in an event the entity is not a trusted entity, the plurality of trust types comprise unknown, public, questionable, and dangerous;

the method further comprising:

determining, at the computing device, a level of access permissions granted in an access control entry (ACE); and

based at least in part on a level of risk of the level of access permission granted in the ACE, issuing a third notification in an event the access permissions exceed a third threshold security level.